ABSTRACT

This invention relates to a conditional access data decryption system, in particular used in the domain of digital pay television.

This system includes a diffusion centre (10) arranged to diffuse data encrypted by control-words (cw), at least one management centre (11) arranged to diffuse personal messages (ECM, EMM) related to the management of access means to encrypted data, an operating device (12) intended to render usable said encrypted data, and a decoder (13) arranged to decrypt at least one part of the encrypted data. This decoder is placed between the diffusion centre (10) and the operating device (12). This decoder (13) comprises a module (14) for the reception and decryption of encrypted data and a module (15) for the management of access rights to this data. The reception module (14) is connected or integrated into the operating device (12) and the management module (15) is arranged to communicate with the reception module. The management module (15) includes a security module (16) arranged to verify the content of the personal messages (ECM, EMM) and to allow or prevent the decryption of the control words (cw) according to the content of the personal messages. The reception module receives the encrypted data originating from the diffusion centre (10) and the management module receives the authorization messages (EMM) from the management centre (11).